

Defeating the Eavesdropper: On the Achievable Secrecy Capacity using Reconfigurable Antennas

Ahmed M. Alaa

Abstract

In this paper, we consider the transmission of confidential messages over slow fading wireless channels in the presence of an eavesdropper. We propose a transmission scheme that employs a single reconfigurable antenna at each of the legitimate partners, whereas the eavesdropper uses a single conventional antenna. A reconfigurable antenna can switch its propagation characteristics over time and thus it perceives different fading channels. It is shown that without channel side information (CSI) at the legitimate partners, the main channel can be transformed into an ergodic regime offering a *secrecy capacity* gain for strict outage constraints. If the legitimate partners have partial or full channel side information (CSI), a sort of selection diversity can be applied boosting the maximum secret communication rate. In this case, fading acts as a friend not a foe.

Index Terms

Channel state information (CSI), outage probability, outage secrecy capacity, reconfigurable antennas, secrecy capacity.

The authors are with XX

Manuscript received XXXX XX, 2013; revised XXXX XX, 201X.

Defeating the Eavesdropper: On the Achievable Secrecy Capacity using Reconfigurable Antennas

I. INTRODUCTION

Information theoretic security was quantified by Shannon's notion of *perfect secrecy*. Perfect information-theoretic secrecy requires the signal received by the eavesdropper not to provide any additional information about the transmitted message [1]. The conventional secret communications scheme includes two legitimate parties, commonly known as Alice and Bob, communicating over a wireless slow fading channel. A malicious third party, known as Eve, eavesdrops on the wireless medium and tries to decode the transmitted signal. In a block fading channel, the channel gain is constant over a codeword, thus the channel is characterized by an outage behavior. The achievable secrecy rate was obtained in terms of the outage probability in [2], where it is shown that for a fading channel, poor secret rates are achieved for strict outage constraints.

Recently, improving the outage secrecy capacity by using multiple antennas has been studied [3] [4] [5]. However, the usage of multiple antennas is inhibited by the space limitations in many wireless transceivers. In addition to that, multiple antennas require multiple RF chains which increases the cost and complexity of the wireless transceiver. In this work, we propose a novel secret communications scheme that employs *reconfigurable antennas*; a class of antennas capable of changing one of its characteristics (polarization, operating frequency and radiation pattern) over time [6] [7] using a single RF chain. Each configuration is known as a *radiation state* and corresponds to an independent channel realization. Previous research work utilized reconfigurable antennas in authentication and secret key generation [8] [9]. However, the achievable capacity bounds for reconfigurable antenna schemes were never obtained before. We propose two modes of legitimate communication via reconfigurable antennas: *state switching* and *state selection*. State switching is applied by the CSI is not available at the transmitter/receiver and relies on switching the antenna *radiation state* over time manipulating the wireless channel and creating artificial channel fluctuations. On the other hand, state selection is applied by selecting the "best" radiation state per codeword for a block fading channel based on the CSI at the transmitter/receiver. It is shown that when strict outage constraints are imposed on the system, state switching can offer an ergodic capacity that exceeds the achievable outage capacity. Moreover, state selection based on partial or full CSI can offer a secrecy capacity that exceeds that of the AWGN channel, thus fading acts as a friend not a foe. State selection resembles opportunistic transmission in a fast fading channel but with power allocation in the *state domain* rather than the time domain, thus supporting both *delay constrained* and *delay tolerant* applications.

As shown in figure 1, we modify the conventional secrecy communications scheme by employing a reconfigurable

antenna at both of the legitimate parties. A message W^k is mapped to a codeword X^n . The codeword is then transmitted from Alice to Bob via a rayleigh fading channel $\gamma_M^n = \{\gamma_M^n(1), \dots, \gamma_M^n(n)\}$, and Additive White Gaussian Noise (AWGN) $= \{n_M^n(1), \dots, n_M^n(n)\}$, where $n_M^n(i) \sim \mathcal{CN}(0, 1)$. The estimated message by the decoder is obtained by demapping the received signal Y_M^n to \hat{W}^k . Eve, an eavesdropper, receives the signal via a similar channel γ_W^n , and noise n_W^n . While Eve uses a conventional single antenna, both Bob and Alice use reconfigurable antennas with Q_R and Q_T propagation modes respectively. The realizations $\gamma_M^n(i)$ and $\gamma_W^n(i)$ are the legitimate and eavesdropper channel realizations for the i^{th} symbol within a codeword of length n . For a slow fading channel, both are constant over a codeword. However, a reconfigurable antenna is capable of switching the channel state once per symbol, thus there are $Q_R Q_T$ possible realizations for the main channel ($\gamma_M^n(i) \in \{\gamma_M(1), \dots, \gamma_M(Q_R Q_T)\}$) and Q_T possible realizations for the eavesdropper channel. Note that all channels are assumed to be Rayleigh fading channels, thus the *probability density functions* (pdfs) of the channels are $f_\gamma(\gamma_M) = \frac{1}{\bar{\gamma}_M} e^{-\frac{\gamma_M}{\bar{\gamma}_M}}$ and $f_\gamma(\gamma_W) = \frac{1}{\bar{\gamma}_W} e^{-\frac{\gamma_W}{\bar{\gamma}_W}}$, where $\bar{\gamma}_W$ and $\bar{\gamma}_M$ are the average SNR values for the main and eavesdropper channels. We define the error probability P_e^n as the average probability of erroneous decoding of the received message, and the equivocation rate R_e as the entropy rate of the transmitted message conditioned on the channel outputs at the eavesdropper, i.e., $R_e \triangleq \frac{1}{n} H(W^k | Y_W^n)$.

Our goal is to maximize both the transmission rate between Alice and Bob in addition to Eve's uncertainty about the message (equivocation rate). A relaxed secrecy condition is letting $\frac{1}{n} H(W^k) - R_e \leq \epsilon$ and $P_e^n \leq \epsilon$, where $\epsilon \rightarrow 0$ as $n \rightarrow \infty$. The secrecy capacity is defined as the maximum achievable secrecy rate for all sequences of $(2^{nR_s}, n)$ codes

$$C_s \triangleq \sup_{P_e^n \leq \epsilon} R_s. \quad (1)$$

The secrecy capacity for AWGN channels (or fixed γ_M and γ_W realizations) is given by

$$C_s = \{\log(1 + \gamma_M) - \log(1 + \gamma_W)\}^+, \quad (2)$$

where $\{x\}^+ = \max\{x, 0\}$. Thus, the AWGN secrecy capacity is given by the difference between legitimate and eavesdropper channel capacities. By defining the outage probability as $P_{out} = P(C_s \leq R_s)$, the ϵ -outage secrecy capacity is the value of R_s that satisfies $P_{out} = \epsilon$.

II. SECRECY CAPACITY OF TRANSMISSION SCHEMES UNDER STUDY

A. Conventional scheme

In this scheme, all parties are using single antennas and the channel is a block fading channel. Assuming that the legitimate and eavesdropper channel realizations are γ_M and γ_W respectively, the secrecy capacity for one realization of both channels is given by (2). For a quasi-static fading channel, we characterize the performance via outage secrecy capacity and outage probability. The outage probability is $P_{out}(R_s) = P(C_s < R_s)$, and can be written as

$$P_{out}(R_s) = P(C_s < R_s | \gamma_M > \gamma_W) P(\gamma_M > \gamma_W)$$

$$+P(C_s < R_s|\gamma_M \leq \gamma_W)P(\gamma_M \leq \gamma_W).$$

From [2] we know that $P(\gamma_M > \gamma_W) = \frac{\bar{\gamma}_M}{\bar{\gamma}_M + \bar{\gamma}_W}$, $P(C_s < R_s|\gamma_M > \gamma_W) = 1 - \frac{\bar{\gamma}_M + \bar{\gamma}_W}{\bar{\gamma}_M + 2^{R_s} \bar{\gamma}_W} e^{-\frac{2^{R_s} - 1}{\bar{\gamma}_M}}$, and $P(C_s < R_s|\gamma_M \leq \gamma_W) = 1$. Thus, the ϵ -outage secrecy capacity is the value of R_s that sets the outage probability to ϵ . The ϵ -outage secrecy capacity R_s is obtained by solving the transcendental equation $(1 - \epsilon)(1 + \frac{\bar{\gamma}_W}{\bar{\gamma}_M} 2^{R_s}) = e^{-\frac{2^{R_s} - 1}{\bar{\gamma}_M}}$, which can be put in a closed-form in terms of the *Lambert W function*. Thus, the ϵ -outage secrecy capacity is given by

$$R_s = \bar{\gamma}_M \times \left\{ \mathcal{W}_o \left(\frac{e^{\frac{1}{\bar{\gamma}_M} + \frac{1}{\bar{\gamma}_W}}}{\bar{\gamma}_W(1 - \epsilon)} \right) - \frac{1}{\bar{\gamma}_W} \right\}^+, \quad (3)$$

where $\mathcal{W}_o(x)$ is the single valued Lambert W function.

B. State switching scheme (Reconfigurable antennas without CSI)

In this scheme, the legitimate transmitter and receiver utilize reconfigurable antennas with Q_T and Q_R radiation states respectively. We assume large codeword lengths and that both Q_T and Q_R are comparable to n . The legitimate channel has $Q_T Q_R$ possible independent realizations per codeword, each realization correspond to a certain transmitter-receiver antenna state selection. We switch the antenna states such that the channel realization changes every symbol within a codeword. A codeword of length n artificially experiences n coherence intervals as long as $n < Q_T Q_R$. Thus, the legitimate channel capacity C_M for specific $Q_T Q_R$ legitimate channel realizations with $Q_T Q_R > n$ is given by $C_M = \frac{1}{n} \sum_{i=1}^n \log(1 + \gamma_M^n(i))$, for $n \rightarrow \infty$ and invoking the *law of large numbers*, we have $C_M = E\{\log(1 + \gamma_M)\}$ where γ_M is an exponential random variable with an average of $\bar{\gamma}_M$. By averaging the legitimate channel capacity over the exponential pdf, the legitimate channel can be defined by an *ergodic capacity* as $C_M = e^{\frac{1}{\bar{\gamma}_M}} \text{Ei} \left(\frac{1}{\bar{\gamma}_M} \right)$ [1], where $\text{Ei}(x) = -\int_{-x}^{\infty} \frac{e^{-t}}{t} dt$ is the exponential integral function. Similarly, the eavesdropper channel has Q_T possible channel realizations, and the eavesdropper channel capacity can be written as $C_W = e^{\frac{1}{\bar{\gamma}_W}} \text{Ei} \left(\frac{1}{\bar{\gamma}_W} \right)$. Therefore, recalling (2), the ergodic secrecy capacity is given by

$$C_s = \left\{ e^{\frac{1}{\bar{\gamma}_M}} \text{Ei} \left(\frac{1}{\bar{\gamma}_M} \right) - e^{\frac{1}{\bar{\gamma}_W}} \text{Ei} \left(\frac{1}{\bar{\gamma}_W} \right) \right\}^+. \quad (4)$$

Note that the ergodic definition for the secrecy capacity in (4) describes two artificial fast fading legitimate and eavesdropper channels. Although the wireless channel is quasi-static, reconfigurable antennas can be used to induce channel fluctuations over time by switching the radiation states to emulate fast fading. We are interested in studying whether the ergodic capacity in (4) can be larger than the ϵ -outage secrecy capacity. Figure 2 depicts the outage secrecy capacity (solid lines) plotted versus ϵ for $\bar{\gamma}_M = 10$ dB together with the ergodic capacity (dashed lines) for different eavesdropper channel average SNR values. Note that the ergodic capacity exceeds the outage capacity for tight outage constraints (i.e. small values of ϵ). For instance, when $\bar{\gamma}_W = -10$ dB, the state switching scheme outperforms the conventional scheme as long as $\epsilon < 0.25$. Moreover, for $\bar{\gamma}_W = 5$ dB, the state switching scheme is better for $\epsilon < 0.4$. Besides, the outage capacity does not exist for $\epsilon < 0.25$, thus the state switching scheme is definitely beneficial for strict outage constraints. On the other hand, when $\bar{\gamma}_M \leq \bar{\gamma}_W$, the ergodic capacity does not exist and only outage capacity with relaxed outage probability constraints is realizable.

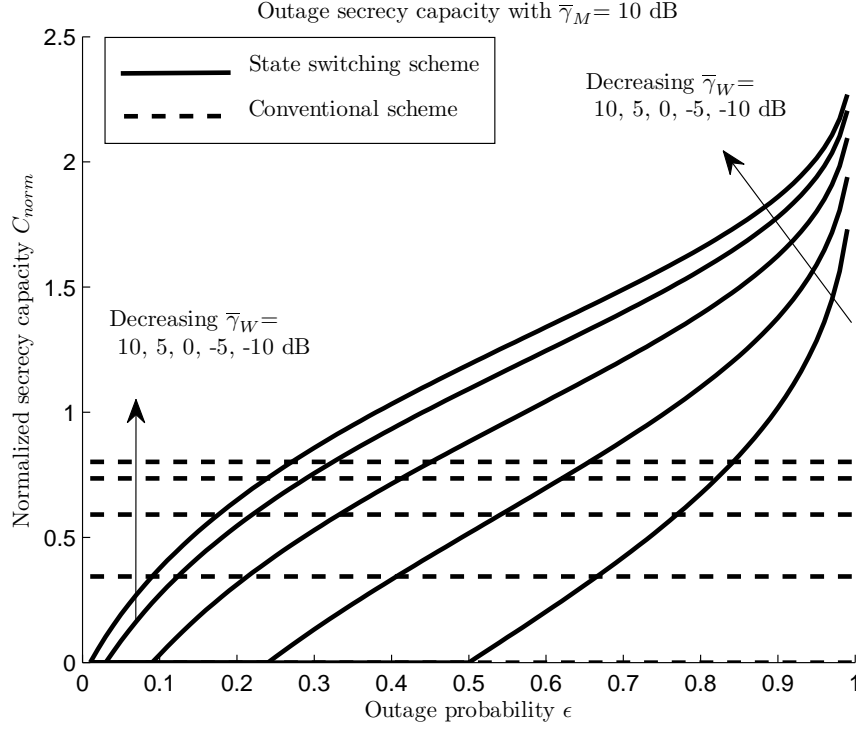


Fig. 1. Outage capacity of the conventional scheme versus the ergodic capacity of the state switching scheme.

C. State selection with partial CSI

In this scheme, the legitimate transmitter has the legitimate channel CSI but is not provided with the eavesdropper channel CSI. Thus, the transmitter and the receiver can agree on the adopted radiation states at both parties once per codeword. The secrecy capacity is given by

$$C_s = \sup_{1 \leq j \leq Q_T Q_R} \left\{ \log(1 + \gamma_{M,j}) - \log(1 + \gamma_W) \right\}^+,$$

where $\gamma_{M,j}$, with $j \in \{1, 2, \dots, Q_R Q_T\}$, is one of the $Q_R Q_T$ independent identical channel realizations obtained by different combinations of the transmission and reception radiation states [7], and γ_W is a Rayleigh random variable and represents the corresponding eavesdropper channel obtained from a certain selection of the radiation states. Intuitively, the secrecy capacity for a certain set of $Q_R Q_T$ channel realizations is given by

$$C_s = \left\{ \log(1 + \gamma_{M,max}) - \log(1 + \gamma_W) \right\}^+, \quad (5)$$

where $\gamma_{M,max} = \max\{\gamma_{M,1}, \gamma_{M,2}, \dots, \gamma_{M,Q_R Q_T}\}$. The pdf of $\gamma_{M,max}$ is [10]

$$f_{\gamma}(\gamma_{M,max}) = Q_T Q_R \sum_{i=0}^{Q_T Q_R} \binom{Q_T Q_R - 1}{i} \frac{(-1)^i}{\bar{\gamma}_M} e^{-\frac{\gamma_{M,max}}{\bar{\gamma}_M / (i+1)}},$$

thus, it can be easily shown that $P(\gamma_{M,max} > \gamma_W) = Q_T Q_R \sum_{i=0}^{Q_T Q_R} \binom{Q_T Q_R - 1}{i} \frac{(-1)^i}{i+1} \frac{1}{1 + \frac{(i+1)\bar{\gamma}_W}{\bar{\gamma}_M}}$, whereas $P(C_s < R_s | \gamma_{M,max} > \gamma_W)$ is given in (6). As demonstrated before, $P_{out}(R_s) = P(C_s < R_s | \gamma_{M,max} > \gamma_W)P(\gamma_{M,max} > \gamma_W) + P(C_s < R_s | \gamma_{M,max} \leq \gamma_W)P(\gamma_{M,max} \leq \gamma_W)$ and the ϵ -outage secrecy capacity is obtained by solving the transcendental equation in (7) for R_s .

$$P(C_s < R_s | \gamma_{M,max} > \gamma_W) = Q_T Q_R \sum_{i=0}^{Q_T Q_R} \binom{Q_T Q_R - 1}{i} \frac{(-1)^i}{(i+1)} \left(\frac{1}{1 + \frac{(i+1)\bar{\gamma}_W}{\bar{\gamma}_M}} - \frac{e^{\frac{-(2R_s-1)(i+1)}{\bar{\gamma}_M}}}{1 + \frac{(i+1)2^{R_s}\bar{\gamma}_W}{\bar{\gamma}_M}} \right). \quad (6)$$

$$\frac{1 - \epsilon}{\left(Q_T Q_R \sum_{i=0}^{Q_T Q_R} \binom{Q_T Q_R - 1}{i} \frac{(-1)^i}{i+1} \frac{1}{1 + \frac{(i+1)\bar{\gamma}_W}{\bar{\gamma}_M}} \right)} = \left(1 - Q_T Q_R \sum_{i=0}^{Q_T Q_R} \binom{Q_T Q_R - 1}{i} \frac{(-1)^i}{(i+1)} \left(\frac{1}{1 + \frac{(i+1)\bar{\gamma}_W}{\bar{\gamma}_M}} - \frac{e^{\frac{-(2R_s-1)(i+1)}{\bar{\gamma}_M}}}{1 + \frac{(i+1)2^{R_s}\bar{\gamma}_W}{\bar{\gamma}_M}} \right) \right). \quad (7)$$

D. State selection with full CSI

Assume that both the legitimate and the eavesdropper channel CSI are available at the legitimate parties. In this case, state selection will be applied such that the legitimate channel is maximized while the eavesdropper channel is minimized. Because the legitimate channel depends on the selection of one of Q_T transmitter radiation states, and one of Q_R receiver radiation states, we have a total of $Q_T Q_R$ possible independent channel realizations. On the other hand, the eavesdropper channel depends only on the transmitter radiation state and thus has one of Q_T possible channel realizations. Let the legitimate channel be denoted by $\gamma_M^{i,j}$ where $i \in \{1, \dots, Q_T\}$ and denotes the selected transmitter radiation state, whereas $j \in \{1, \dots, Q_R\}$ and denotes the selected receiver state. Similarly, the eavesdropper channel is γ_W^i where $i \in \{1, \dots, Q_T\}$, thus we note that the selection of a transmitter radiation state dictates an eavesdropper channel and a set of possible Q_R legitimate channels, from where a single realization is picked based on the receiver state. The achievable secrecy capacity for a certain set of legitimate and eavesdropper channel realizations corresponds to the supremum of all selections for transmitter and receiver radiation states

$$C_s = \sup_{1 \leq i \leq Q_T, 1 \leq j \leq Q_R} \left\{ \log(1 + \gamma_M^{i,j}) - \log(1 + \gamma_W^i) \right\}^+. \quad (8)$$

Equation (8) suggests that we do not only improve the legitimate channel, but also use the CSI to select the radiation state that undermines the eavesdropper channel. Numerical results for the ϵ -outage secrecy capacity R_s are obtained in section IV.

III. NUMERICAL RESULTS

In figure 3, we investigate the achievable ϵ -outage secrecy capacity for different schemes. By setting $\epsilon = 0.1$, we plot the secrecy capacity versus $\bar{\gamma}_M$ for low and high values of $\bar{\gamma}_W$ (-10 and 20 dB respectively). Note that adopting single antennas (conventional scheme) causes an SNR loss of around 10 dB for $\bar{\gamma}_W = 20$ and -10 dB compared to the AWGN secrecy capacity. Reconfigurable antennas provide considerable SNR gains when the CSI is available.

Without CSI, the state switching scheme provides poor ergodic capacity for $\bar{\gamma}_W = 20$ dB. For $\bar{\gamma}_W = -10$ dB, the ergodic capacity of the state switching scheme outperforms the outage capacity of the conventional single antenna system for $\bar{\gamma}_M < 25$ dB. In this case, an SNR gain of about 5 dB is achieved. Thus, the state switching scheme offers an SNR gain only for low values of $\bar{\gamma}_M$. On the other hand, the state selection with partial CSI scheme offers a significant gain for all legitimate and eavesdropper SNR ranges. The number of radiation states involved in calculations are $Q_T = Q_R = 5$. For $\bar{\gamma}_W = -10$ dB, partial CSI offer 5 dB SNR gain compared to the AWGN capacity and 15 dB compared to the single antenna system in Rayleigh fading. For high eavesdropper average SNR ($\bar{\gamma}_W = 20$ dB), an SNR gain of 2 dB compared to the AWGN capacity and 12 dB compared to the conventional scheme. It is worth mentioning that the achievable gain is higher for lower values of $\bar{\gamma}_W$ as this scheme is not provided with the eavesdropper channel CSI. Moreover, the state selection scheme with full CSI provide superior secrecy capacity compared to all other schemes. This gain is most notable for large $\bar{\gamma}_W$, i.e. for $\bar{\gamma}_W = 20$ dB, where and SNR gain of 20 dB compared to the AWGN capacity and 30 dB compared to the single antenna fading channel capacity. The reason for such impressive performance boost is that knowledge of the eavesdropper CSI and the selection of the “worst” eavesdropper channel is most effective when the eavesdropper channel enjoys high SNR. The gain achieved for $\bar{\gamma}_W = -10$ dB is about 8 dB compared to the AWGN channel. The gain decreases for low values of $\bar{\gamma}_W$ because undermining the eavesdropper channel becomes of less effectiveness.

Figure 4 demonstrates the secrecy capacity normalized to the AWGN secrecy capacity for $\epsilon = 0.1$ and $\bar{\gamma}_W = -10, 0$ and 10 dB. Focusing on the state selection scheme with full CSI, we note that the capacity gain is maximum at low SNR. This is similar to the effect of optimal water filling power allocation over a fast fading channel, where the highest capacity gain is obtained at low SNR. In our case power allocation is applied across the radiation state domain rather than the time domain. Besides, instead of water filling, we allocate all power to the best radiation state. Thus, we are able to achieve considerable capacity gains regardless of the time latency of the applications, i.e. delay tolerant and delay sensitive applications are both supported by the reconfigurable antenna scheme.

REFERENCES

- [1] P. K. Gopala, L. Lai and H. El Gamal, “On the Secrecy Capacity of Fading Channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4697, Oct. 2008.
- [2] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, pp. 356-360, Jul. 2006.
- [3] A. Khandani, G. Bagherikaram, and A. Motahari, “The Secrecy Capacity Region of the Gaussian MIMO Broadcast Channel,” *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2673-2682, Oct. 2013.
- [4] A. Khisti and G. W. Wornell, “Secure Transmission With Multiple Antennas?art II: The MIMOME Wiretap Channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Oct. 2010.
- [5] C. Y. Wu, P. C. Lan, P. C. Yeh, C. H. Lee and C. M. Cheng, “Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices,” *IEEE J. Selected Areas Commun.*, vol. 31, no. 9, pp. 1687-1700, Sept. 2013.
- [6] Yaxing Cai and Zhengwei Du, “A Novel Pattern Reconfigurable Antenna Array for Diversity Systems,” *IEEE Antennas and Wireless Propagation Letters*, vol. 8, pp. 1227-1230, 2009.
- [7] P. A. Martin, P. J. Smith, and R. Murch, “Improving Space-Time Code Performance in Slow Fading Channels using Reconfigurable Antennas,” *IEEE Communications Letters*, vol. 16, pp. 494-497, Apr. 2012.

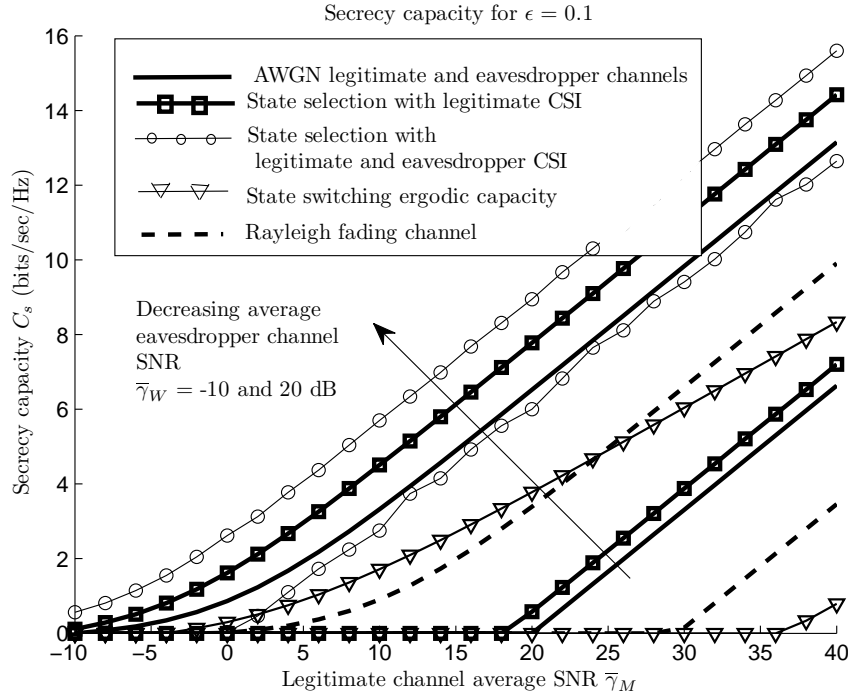


Fig. 2. Comparison between all secret communications schemes.

- [8] P. Mookiah and K. R. Dandekar, "A Reconfigurable Antenna-Based Solution for Stationary Device Authentication in Wireless Networks," *International Journal of Antennas and Propagation*, vol. 2012, Article ID 545783, 11 pages, 2012.
- [9] R. Mehmood, and J. W. Wallace, "Wireless security enhancement using parasitic reconfigurable aperture antennas," *Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP)*, Rome, pp. 2761-2765, April 2011.
- [10] Ning Kong, "Performance Comparison among Conventional Selection Combining, Optimum Selection Combining and Maximal Ratio Combining," *Proceedings of IEEE International Conference on Communications (ICC'09), Dresden, Germany*, pp. 1-6, June 2009.

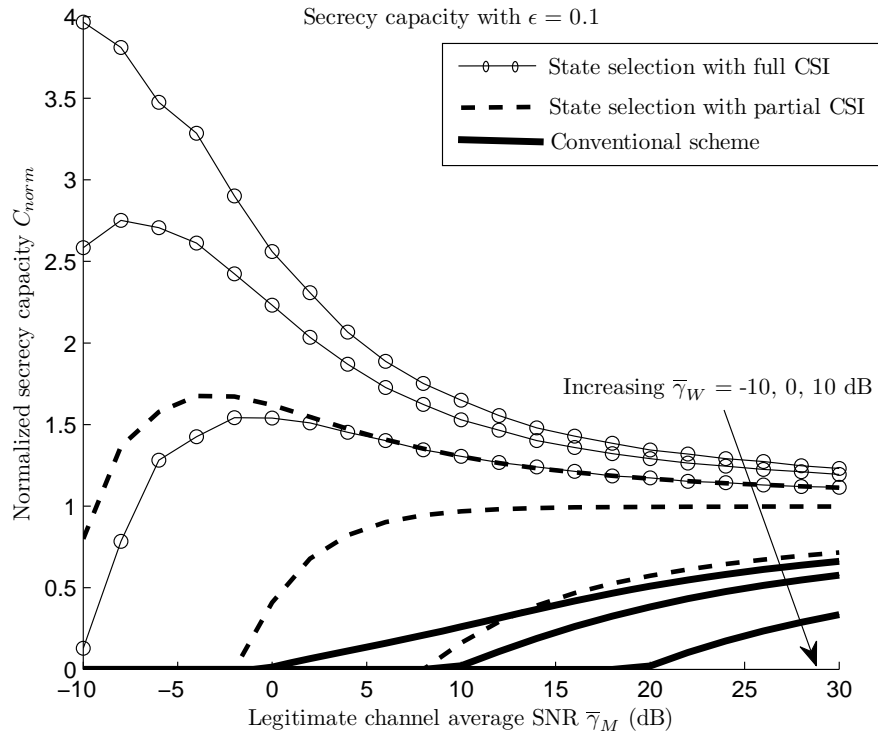


Fig. 3. Secrecy capacity gain for different schemes.